How hackers can without you knowing

Kurt Knutsson, CyberGuy Report

There is enough to worry about in life without the additional stress and terror of finding out your friends, family or complete strangers have been receiving a text message from "you" without your knowledge. How did they do that? How did they send a text message from your phone without you knowing?
This is a real threat that many people face every day. That's why we felt it was so important to answer this question sent in from John.

"I just found a text written to me, which was a response to a text I sent. ***Problem is, I didn't send the text****? I'm 65 years old, and not as spry as I once was, but I do not remember sending the text. My wife is trying to convince me I'm going crazy. She says it's impossible for someone to send a text (impersonating me) without having possession of my phone. Is that true? Can someone hack your phone and send text??" –* ***John, Fort Myers, FL***

We're sorry to hear that you're going through this, John. It is possible for someone to send a text message impersonating you without having possession of your phone. This is known as **SMS spoofing**, and it is a technique used by cybercriminals to send fraudulent text messages.

SMS spoofing works by manipulating the sender ID of a text message to make it appear as if it was sent from a different phone number. This can be done using various online services that **allow users to send text messages with a fake sender ID.** Cybercriminals will change the sender ID to impersonate friends, family, or a legitimate company.

It is important to note that **SMS spoofing is illegal and can be used for malicious purposes** such as phishing scams, identity theft, and fraud. Scammers bank on the combination of familiarity and urgency to get you to interact with their text either by clicking on a link, downloading a file, or responding with personal information.

Here are the top 3 reasons why scammers often send text messages under a fake sender ID with some urgent request:

1. **Trick you into clicking on a malicious link** that leads you to a malicious website to rob you of your personal or financial information or even unleash malware or viruses to your phone.
2. **Lure you into paying a fake bill** under the guise of a reputable or familiar company.
3. **Damages your reputation or relationship** with friends, family, and others by sending harmful messages.

In the past, many Apple devices were considered to be virtually immune to viruses and malware. Unfortunately, due to bugs in iOS, hackers can take over someone's device just like any other device on the market. While Apple patches these vulnerabilities on a consistent basis, this **leaves iPhone users vulnerable to SMS spoofing, too.**

A hacker can use "interaction-less" bugs to send a specially crafted SMS message and the iMessage server can send user-specific data, including images or SMS messages, back to them. **The user doesn't even have to open the messages to activate this bug**. Additionally, **hackers can send malicious codes through texts**, embedding them onto the user's phone. These vulnerabilities are **unique to Apple devices**.

Aside from the specific vulnerabilities, hackers generally **need the user to interact with the text message before the malicious code gets unleashed onto the device.**

If you suspect that your phone has been hacked or that someone is impersonating you, it is important to **take immediate action. Here are some steps you can take:**

1) Have good antivirus software on your phone: Having good antivirus software actively running on your devices will alert you of any malware in your system, warn you against clicking on any malicious links that may install malware on your devices, allowing hackers to gain access to your personal information. Find my review of Best Antivirus Protection here.

2) Keep your phone software updated: Both iPhone and Android users should keep their phone's OS and apps updated regularly as Apple and Google release patches to vulnerabilities as they are discovered. Updating your phones can prevent hackers from exploiting security flaws and sending text messages from your phone without you knowing.

3) Change your passwords: Change the passwords for all your online accounts, including your email, social media, and banking accounts. Do not use easy-to-guess information such as your birthday or address. Use strong, unique passwords that are difficult to guess; preferably ones that are alphanumeric and, if applicable, include special symbols. Be sure to do this on another device in case there is malware on your phone monitoring you. Consider using a password manager to generate and store complex passwords. It will help you to create unique and difficult-to-crack passwords that a hacker could never guess.

4) Enable two-factor authentication: Enabling two-factor authentication on all your online accounts will add an extra layer of security to your accounts and make it more difficult for hackers to gain access.

5) Contact your mobile carrier: Contact your mobile carrier and report the incident. They may be able to help you identify the source of the text message and take appropriate action.

6) File a police report: If you believe that you have been a victim of identity theft or fraud, file a police report with your local law enforcement agency.

7) Watch your connections: When possible, **do not connect to unprotected or public Wi-Fi hotspots** or Bluetooth connections. Turn off the Bluetooth connection when not in use. On most iPhones, you can choose who to receive files or photos via AirDrop (a Bluetooth feature) from by selecting to receive from "no one," people in your Contacts, or Everyone. We suggest you set it to "no one" and **only turn it on when you are with the person you are sending or receiving a file or photo from.**

Below are some next steps if you find you or your loved one is a victim of identity theft from an SMS spoofing attack.

1) Change your passwords. If you suspect that your phone has been hacked or that someone is impersonating you, they could access your online accounts and steal your data or money. ON ANOTHER DEVICE (i.e., your laptop or desktop), you **should change your passwords for all your important accounts, such as email, banking, social media, etc.** You want to do this on another device so the hacker isn't' recording you setting up your new password on your hacked device. Use strong and unique passwords that are hard to guess or crack. You can also consider using a password manager to generate and store your passwords securely.

2) Look through bank statements and check account transactions to see where outlier activity started.

3) Use a fraud protection service. Identity Theft companies can monitor personal information like your Social Security Number (SSN), phone number, and email address and alert you if it is being sold on the dark web or being used to open an account. They can also assist you in freezing your bank and credit card accounts to prevent further unauthorized use by criminals.

Some of the best parts of using an identity theft protection service include identity theft insurance to cover losses and legal fees and a white glove fraud resolution team where a U.S.-based case manager helps you recover any losses. See my tips and best picks on how to protect yourself from identity theft.

4) Report any breaches to official government agencies like the Federal Communications Commission.

5) You may wish to get the professional advice of a lawyer before speaking to law enforcement, especially when you are dealing with criminal identity theft, and if being a victim of criminal identity theft leaves you unable to secure employment or housing

6) Alert all three major credit bureaus and possibly place a fraud alert on your credit report.

7) Run your own background check or request a copy of one if that is how you discovered your information has been used by a criminal.

8) Alert your contacts. If hackers have accessed your device through SMS spoofing, they could use it to send spam or phishing messages to your contacts. They could impersonate you and ask for money or personal information. You should alert your contacts and warn them not to open or respond to any messages from you that seem suspicious or unusual.

9) Restore your device to factory settings. If you want to make sure that your device is completely free of any malware or spyware, you can restore it to factory settings. This will erase all your data and settings and reinstall the original version. You should back up your important data BEFORE doing this, and only restore it from a trusted source.

If you are a victim of identity theft, the most important thing to do is to take immediate action to mitigate the damage and prevent further harm.

MORE: HOW TO TELL IF SOMEONE HAS READ YOUR TEXT MESSAGE

It’s possible for someone who doesn’t have physical possession of your phone to spoof your information for SMS spoofing. Though you might not have control over who gets your number, there are steps you can take to protect yourself.

Have you ever received a convincing text spoof message? What were the telltale signs that it was a spoofed message? Let us know by writing us at Cyberguy.com/Contact.